19

AUSA: Kevin Mulcahy Telephone: (313) 226-9713

AO 91 (Rev. 11/11) Criminal Complaint Special Agent: Raymond C. Nichols Telephone: (313) 496-4353

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

United States of America
v.
Buster Jimmy Hernandez

Case:2:19-mj-30214
Judge: Unassigned,
Filed: 04-29-2019 At 02:47 PM
USA v. BUSTER JIMMY HERNANDEZ(CMP)(MLW)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 2012 - June 2017 in the county of Wayne in the Eastern District of Michigan, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2251(a)(e)	Producing and attempting to produce child pornography
18 U.S.C. § 2422	Coercion and enticement
18 U.S.C. § 875	Threats to injure

This criminal complaint is based on these facts:

See attached Affidavit

☐ Continued on the attached sheet.

Complainant's signature

Raymond C. Nichols, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/29/2019

Judge's signature

City and state: Detroit, Michigan

Anthony P. Patti, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR COMPLAINT AND ARREST WARRANT

I. Introduction

I, Raymond C. Nichols, having been first duly sworn, do hereby depose and state as follows:

1. I have been employed as a Special Agent of the FBI since February 2012, and am currently assigned to the FBI Detroit Division. Prior to being employed by the FBI I obtained a bachelor's degree in computer information systems and was employed as a network/server administrator for approximately 9 years. While employed by the FBI, I have investigated federal criminal violations related to Internet fraud, computer intrusions, and the FBI's Innocent Images National Initiative, which investigates matters involving the online sexual exploitation of children. I have gained experience through training at the FBI Academy, post Academy training, and everyday work related to conducting these types of investigations.

2. This affidavit is made in support of an application for a criminal complaint and arrest warrant for **BUSTER JIMMY HERNANDEZ** (date of birth **/**/1990) for violations of: 18 U.S.C. § 2251(a) and (e) (producing and attempting to produce child pornography); 18 U.S.C. § 2422 (coercion and enticement) ; and 18 U.S.C. § 875 (threats to injure) (collectively hereinafter referred to as the "SUBJECT

OFFENSES").

3. The statements contained in this affidavit are based in part on: written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; independent investigation and analysis by law enforcement officers/analysts and computer forensic professionals; and my experience, training and background as a Special Agent (SA) with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested arrest warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause that **HERNANDEZ** has violated Title 18 U.S.C. § 2251(a) and (e); 18 U.S.C. § 2422; and 18 U.S.C. § 875.

II. Background Information Concerning the Internet, Internet Protocol Addresses, and the TOR Network

4. Law enforcement agents and I have learned the following about the Internet, Internet Protocol Addresses, and the Tor anonymity network:

5. The Internet is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information

sent between two computers connected to the Internet frequently cross state and international borders even when the two computers are located in the same state.

6. Internet Service Providers ("ISPs"): Most individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each ISP.

7. Internet Protocol Address ("IP address"): The Internet Protocol Address is a unique numeric address used to identify computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer (or group of computers using the same account to access the Internet) attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. An IP address acts much like a home or business street address – it enables Internet sites to properly route traffic to each other. There are two types of IP addresses – dynamic and static.

8. Dynamic IP address. Most of the larger ISPs such as Comcast or AT&T control blocks of IP addresses to assign their customers. Although there may be thousands of IP addresses within these blocks, there are not enough to enable larger ISPs to assign one, permanent IP address to each of their millions of customers. Therefore, these ISPs use dynamic IP addressing: Each time a user dials into the ISP to connect to the Internet, the ISP randomly assigns to that customer one of the available IP addresses in the range (or block) of IP addresses controlled by the ISP. The customer's computer retains that IP address for the duration of that session alone. Once he disconnects from the Internet, that IP address becomes available to other customers who dial in at a later time.

9. Static IP address. A static IP address is an IP address that is assigned permanently to a given computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time. Customers who are connected to the Internet via high-speed cable or Digital Subscriber Lines (DSL) are often assigned static IP addresses because their computers have full-time Internet access. In this case, the Target Subscriber is a static IP address that is assigned to a DSL line connected to a computer located in the Los Angeles, California area.

10. Domain Name System: IP addresses generally have corresponding domain names; the Domain Name System ("DNS") is an Internet service that maps

domain names, such as the domain name "cybercrime.gov," to their corresponding IP address (e.g., 128.121.13.121). This mapping function is performed by DNS servers located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

11. File Transfer Protocol ("FTP") is a communication protocol for transferring files between computers connected to the Internet.

12. Ports: All computers connected to the Internet have 65,535 available ports through which electronic communications could enter or exit, depending on the computer's configuration. There are agreed-upon standard ports used for common types of communications. For instance, most computers are configured to send and receive web messages on port 80; e-mail traffic on port 25; and file transfers via file transfer protocol (FTP) on port 21. Therefore, in addition to directing an electronic communication to a particular IP address, an Internet user (or computer) may also designate the port of the computer assigned that IP address through which the electronic communication should enter.

13. Log Files are computer files containing information regarding the activities of computer users, processes running on a computer and the activity of computer resources such as networks, modems, and printers.

14. The Tor network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.

15. Use of the Tor software bounces a user's communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable.

16. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that Tor exit node IP address.

17. A criminal suspect's use of Tor accordingly makes it extremely difficult for law enforcement agents who are investigating a Tor Hidden Service to detect the users' actual IP addresses or physical locations.

18. Similarly, an anonymous proxy is defined as a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an

intermediary and privacy shield between a client computer and the rest of the Internet.

19. Finally, 4chan is an English-language image board website. 4chan is split into various boards with their own specific content and guidelines. 4chan has a registration system that allows users to post on the board anonymously. If a user posts without creating a nickname, the post is automatically attributed to "Anonymous." Accordingly, the general understanding on 4chan is that "Anonymous" is not a single person, but rather, a collective of users.

20. Based on my training and experience, users choose 4chan because it allows for anonymous message boarding. As set forth above, because registration is not required, specific posts cannot be attributable or traceable to a particular individual. As a result, numerous topics are discussed on 4chan, including topics that concern illegal activities such as sexual interest in children, terrorist activities, and illicit drug distribution.

III. Background of Investigation

21. The Defendant, **BUSTER JIMMY HERNANDEZ** (hereinafter "Hernandez" or "the Defendant"), was a resident of Bakersfield, California, who was born in 1990. As explained in more detail below, Hernandez is currently facing multiple charges of child exploitation and threat offenses in a superseding indictment in the Southern District of Indiana related to Victim 1 and Victim 3, both from Indiana.

The charges in the Southern District of Indiana stem from a months-long series of threatening and extortive posts made by Hernandez (using the moniker "Brian Kil") to Victim 1. Hernandez threatened to commit a school shooting at Victim 1's high school, posted child pornography images of Victim 1 that he extorted from her, and promised to shoot law enforcement who attempted to stop his threatened school shooting.

22. Victim 2 was a female living in Brownstown Charter Township, Michigan (Wayne County), who was born in September 1997.

23. Since in or around December 2015, law enforcement has been investigating the criminal activities of an unknown subject known most frequently as "Brian Kil." As set forth in more detail below, I believe that the unknown subject using the moniker "Brian Kil", and others, has victimized minors in at least ten federal districts. I further believe, based upon my training and experience, and the investigation in this case, that "Brian Kil" is **BUSTER JIMMY HERNANDEZ**.

24. Based on the investigation to date, "Brian Kil" uses the following methods to obtain or attempt to obtain child pornography:

a. Using various social medial accounts, "Brian Kil" contacts random individuals (typically minors) by sending a private message, and saying,

for example, "Hi 'Victim Name,' I have to ask you something. Kinda important." "Brian Kil" then asks the prospective victim, "How many guys have you sent dirty pics to cause I have some of you?" The prospective victim either ignores "Brian Kil" or engages in further conversation.

b. If the potential victim responds, "Brian Kil" tells her to send more nude/sexually explicit images or videos to him, or he would send the nude/sexually explicit images or videos allegedly in "Brian Kil's" possession to the potential victim's friends and family (also known as "sextortion").

c. According to a multi-district investigation, numerous victims (including minor victims) have complied with "Brian Kil's" demands and have sent him images and videos depicting the victims engaging in sexually explicit conduct. Once he receives the images and videos, "Brian Kil" continues to extort the victim, until she refuses to comply. At that point, "Brian Kil" typically posts the sexually explicit images or videos of the victim online, or sends them to the victim's friends and family via the Internet.

d. In each instance, "Brian Kil" has, until now, successfully masked the

true location of his Internet Protocol ("IP") address by using the Tor Network.

25. Between, in or about 2012 and June 2017, Kil, using multiple aliases known to investigators and related to the "Brian Kil" moniker, communicated with Victim 2, who is known to investigators, (and who is now no longer a minor), using Twitter, text messages, and Dropbox.com.

26. Throughout the exchanges (including when Victim 2 was a minor), Kil threatened to post nude images and videos of Victim 2 online unless he/she sent Kil images and videos consisting of child pornography. In response, Victim 2 sent Kil multiple images and videos containing visual depictions of Victim 2 engaging in sexually explicit activity that, until he/she reached the age of majority, constituted child pornography. On each occasion, Kil's IP address was masked using the Tor network. Investigators were unable to locate any true IP addresses for Kil's computer. Consequently, Kil's physical location was impossible to determine.

27. Kil has also instructed Victim 2 to upload images and videos to a Dropbox.com account known to investigators. The Dropbox.com account is not publicly accessible. Descriptions of multiple images sent to Kil are as follows:

a. On or about January 20, 2015, Victim 2 sent Kil an image file titled IMG_0238.jpg. The image file consists of the visual depiction of Victim 2's

body. Her face is not visible. Victim 2 is shown from the neck down completely nude. She is shown gripping her left breast with her left hand. The picture appears to be located in a bathroom. A pink hairbrush is visible behind her.

b. On or about October 6, 2014, Victim 2 sent Kil a video file at Kil's request. The video file consists of Victim 2 standing in a bedroom with her face and body fully visible. She is shown wearing yellow underwear and a black shirt. Victim 2 is then shown removing her underwear and shirt, exposing her breasts and vagina. She then approaches the camera and turns it off.

IV. Identifying Brian Kil

28. On June 9, 2017, the Honorable Debra McVicker Lynch of the Southern District of Indiana, authorized the execution of a Network Investigative Technique "NIT" (defined in Cause No. 1:17-mj-437) in order to ascertain the IP address associated with Brian Kil and Victim 2. As set forth in the search warrant application presented to Judge Lynch, the FBI was authorized by the Court to add a small piece of code (NIT) to a normal video file produced by Victim 2, which did not contain any visual depictions of any minor engaged in sexually explicit activity. As authorized, the FBI then uploaded the video file containing the NIT to the Dropbox.com account

known only to Kil and Victim 2. When Kil viewed the video containing the NIT on a computer, the NIT would disclose the true IP address associated with the computer used by Kil.

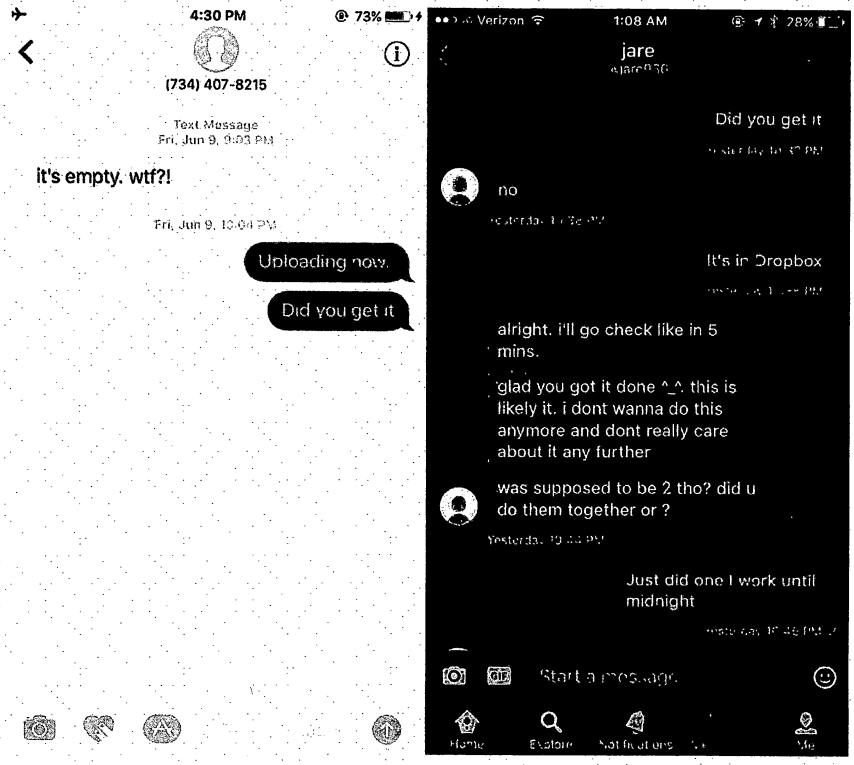
29. On June 9, 2017, FBI agents interviewed Victim 2 at her residence in Michigan. According to Victim 2, Kil began demanding sexually explicit images and videos from him/her in on or about in or about 2012. Since then, and while Victim 2 was still a minor, she complied under duress, and sent Kil numerous videos and images of child pornography. According to Victim 2, Kil threatened Victim 2 stating that if she/he did not comply with Kil's demands, he/she would post sexually explicit images and videos of Victim 2 online and send them to his/her family and friends.

30. According to Victim 2, on or about June 9 (the same date of the interview) Kil demanded that she send sexually explicit videos to a Dropbox account Kil created. Kil sent this demand from the telephone number (734) ***-8215. The phone number (734) ***-8215 is registered to bandwidth.com. Numbers registered to bandwidth.com are voice over IP Voicer over Internet Protocol (VOIP) numbers. VOIP is a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions. The subject communicating with

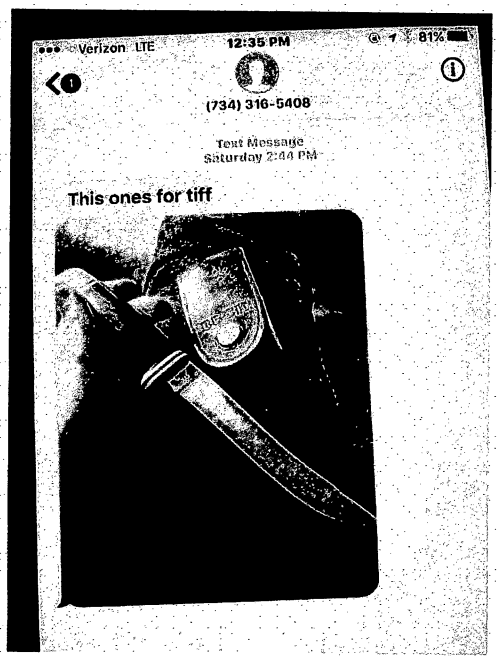
Victim 2 and her family used Tor to obfuscate all communications with victims. Accordingly, the real subscriber was not locatable.

31. On June 9, 2017, after interviewing Victim 2, the FBI executed the search warrant and used the NIT to identity the masked IP addressed used by Kil. After the NIT was uploaded to Dropbox, the FBI told Kil it was available by communicating with the (734) ***-8215 number and a Twitter.com account identified by Victim 2 as belonging to the same person who was extorting her.

32. Screenshots of the communications follow:



33. After receiving the video, Kil then began sending messages to the family of Victim 2 stating that Kil was going to murder members of her family (see screenshot below):



34. When Kil viewed the video containing the NIT on a computer, the NIT disclosed the true IP address associated with the computer used by Kil. Subpoena results of the true IP address led to Hernandez's residence in Bakersfield, California. Further investigation, including database checks, social media checks, pen register/trap and trace on the true IP address, and use of a pole camera all connected Hernandez to the Bakersfield, California address where Hernandez resided with his girlfriend.

35. On July, 17, 2017, United States District Judge Tonya Walton-Pratt authorized the interception of communications to and from that true IP address ("Title III Wiretap"). The following are some of the pertinent communications intercepted:

a. On July 22, 2017, the user of the IP account viewing 4chan, viewed a photograph of the Columbine killers in the cafeteria of the school. This photograph is significant because" Brian Kil" posted this photograph on Tumblr when he threatened a school district in 2015.

b. On July 17, 2017, the user of the IP account viewing "imgur," viewed a photograph depicting what appears a very young female, lying on her back, with a white fluid on her chest and stomach (presumably semen).

c. Additionally, law enforcement data containing intercepted multiple photographs of young females in various stages of undress. Agents are working to determine whether any of the females depicted in the photographs have been previously identified as Brian Kil's victims of sextortion.

36. A review of the Tor usage records from the Title III wiretap and the pole camera data showed that Tor was accessed almost continuously when Hernandez's girlfriend was not at the residence. Additionally, **BUSTER HERNANDEZ** was

always present when the Tor Network was utilized as observed via the interceptions set forth in paragraph 35.

37. On August 3, 2017 a search warrant was executed at the residence of **BUSTER HERNANDEZ** in Bakersfield, California. During the search warrant law enforcement recovered a USB device that contained an operating system specifically designed for anonymity. When removed from a computer or powered down, the operating system on the USB device would not retain any evidence of actions taken by the user. The USB device was also designed to leave no trace on the computer used to run it. The discovery of this operating system is pertinent because the NIT, described in paragraph 28, and deployed as described in paragraph 31, was designed to only target this operating system. Your affiant notes that as described above the NIT was successful in obtaining the true IP address used by **BUSTER HERNANDEZ**.

38. Also, during the search warrant on August 3, 2017 an encrypted hard disk drive was recovered. Due to the encryption used on the hard disk drive law enforcement has not been able to recover or review the data contained on it.

39. During the execution of the search warrant on August 3, 2017 **BUSTER HERNANDEZ'** live in girlfriend was interviewed by the FBI. The girlfriend told the FBI that **HERNANDEZ** did not leave their home very often or have friends over.

Additionally, she described **HERNANDEZ'** computer knowledge as a "10" on a 1-10 scale.

40. On September 7, 2017, a grand jury charged **BUSTER HERNANDEZ** with 26 counts of Production and Distribution of Child Pornography, Threats to Use Explosive Devices, and Threats to Injure, in the Southern District of Indiana. On April 9, 2019, **HERNANDEZ** was charged in a superseding indictment with 41 counts of Production and Distribution of Child Pornography, Coercion and Enticement of Minors, Extortion, Threats to Use Explosive Devices, Threats to Injure, Witness Tampering, Witness or Victim Retaliation, and Obstruction of Justice, in the Southern District of Indiana, in Case Number: 1:17-CR—183, before the Honorable Tayna Walton Pratt. Trial is scheduled for August 19, 2019.

Conclusion

41. Based on the foregoing, there is probable cause to believe **BUSTER JIMMY HERNANDEZ** has violated: 18 U.S.C. § 2251(a) and (e) (producing and attempting to produce child pornography); 18 U.S.C. § 2422 (coercion and enticement); and 18 U.S.C. § 875 (threats to injure).

Special Agent Raymond C. Nichols
Federal Bureau of Investigation

Sworn to me this 29th day of April, 2019

Anthony P. Patti
United States Magistrate Judge